UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/885,427	06/19/2001	Peter A.J. van der Made	81924.0002	4888

7590 07/20/2005

W SCOTT PETTY
KING & SPALDING
191 PEACHTREE STREET 45TH FLOOR
ATLANTA, GA 30303-1763

EXAMINER	
GUILL, RUSSELL L	
ART UNIT	**PAPER NUMBER**
2123	

DATE MAILED: 07/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/885,427	MADE, PETER A.J. VAN DER	
	Examiner	Art Unit	
	Russell L. Guill	2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 - 10 were cancelled. Claims 11 - 30 were added. Claims 11 - 30 have been examined. Claims 11 - 30 have been rejected.

Response to Applicant's Remarks

2. Because claims 1 - 10 have been cancelled, the issues with the original claims are moot.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3.1. Claim 27 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 27 recites, "loading a software CPU shell when the virtual machine operates in the first and second modes of operation". The second mode of operation uses a high level language, and the specification does not appear to support loading a software CPU shell in this case.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 11 - 16, 18 - 25 and 27 - 30 are is rejected under 35 U.S.C. 103(a) as being unpatentable over Le Charlier (Le Charlier, Badouin; Swimmer, Morton; Mounji, Abdelaziz; "Dynamic Detection and Classification of Computer Viruses using General Behavior Patterns", 1995, Proceedings of the Fifth International Virus Bulletin Conference, Boston), in view of Custer (Custer, Helen; "Inside Windows NT", 1993, Microsoft Press), further in view of Chi (U.S. Patent 5,978,917; November 2, 1999).

5.1. Regarding claim 11:

5.1.1. Le Charlier teaches:

5.1.1.1. a virtual machine to execute a target program for virus detection (***pages 1 - 2, Abstract; and page 13, section 4.4 8086 emulation***).

5.1.1.2. storing behavior flags representing behavior of the target program during execution of the target program by the virtual machine (***pages 13 - 14, section 4.5 Activity Data Format; and page 14, figure 3***).

5.1.1.3. storing a sequence in which the behavior flags are set by the target program during execution of the target program by the virtual machine (***pages 13 - 14, section 4.5 Activity Data Format; and page 14, figure 3***).

5.1.1.4. passing behavior flag data and sequence flag data from the virtual machine to the computer system for evaluation after execution of the target program by the virtual machine (***pages 14 - 15, section 4.6 Activity Data Collection***).

5.1.1.5. terminating the virtual machine after execution of the target program, thereby removing from the computer system a copy of the target program that was contained within the virtual machine (***pages 13 - 15, sections 4.4 - 4.6***).

5.1.1.5.1. Regarding machine (***pages 13 - 15, sections 4.4 - 4.6***); it is obvious that the virtual machine terminates machine after execution of the target program, thereby removing from the computer system a copy of the target program that was contained within the virtual machine.

5.1.2. Le Charlier does not specifically teach:

5.1.2.1. evaluating a file format of the target program.

5.1.2.2. evaluating control fields within a header of a file containing the target program.

5.1.2.3. automatically configuring the virtual machine to execute the target program in one of three modes of operation based on the file format and the control fields within the header of the file, a first mode of operation comprising a real mode, a second mode of operation for executing target programs comprising a high level programming language, and a third mode of operation comprising a protected mode for executing target programs comprising thirty-two bit code.

5.1.3. Custer teaches:

5.1.3.1. evaluating a file format of the target program, evaluating control fields within a header of a file containing the target program, and automatically configuring ***the machine*** to execute the target program in one of ***two*** modes of operation based on the file format and the control fields within the header of the file, a first mode of operation comprising a real mode, and a third mode of operation comprising a protected mode for executing target programs

comprising thirty-two bit code (*pages 133 – 135, section 5.2.2 Running Applications; and page 134, figure 5-11; and page 149, section 5.4.1 Virtual DOS Machines*).

5.1.3.1.1. Regarding (*pages 133 – 135, section 5.2.2 Running Applications; and page 134, figure 5-11; and page 149, section 5.4.1 Virtual DOS Machines*); since Windows NT runs both Win32 and DOS applications by examining the image file, it would have been obvious to evaluate a file format of the target program, evaluate control fields within a header of a file containing the target program, and automatically configure the machine to execute the target program in one of two modes of operation based on the file format and the control fields within the header of the file, a first mode of operation comprising a real mode, and a third mode of operation comprising a protected mode for executing target programs comprising thirty-two bit code

5.1.4. The motivation for using the art of Custer with the art of Le Charlier would have been obvious given the benefit recited in Custer that one operating system could run different types of programs (*page 115, paragraph 3, "The idea that one . . . "*).

5.1.5. Chi teaches a mode of operation for executing target programs comprising a high level programming language (*figure 1; figure 3; figure 4; and column 1, lines 45 – 58; and column 5, lines 20 - 50*).

5.1.6. The motivation for using the art of Chi with the art of Le Charlier would have been obvious given the benefit recited in Chi of an ability of the invention to detect and eliminate viruses in a generic manner (*column 2, lines 60 – 64*). Therefore, as discussed above, it would have been obvious to the ordinary artisan at the time of invention to use the art of Custer and Chi with the art of Le Charlier to produce the claimed invention.

5.2. Regarding claim 12:

5.2.1. Le Charlier teaches evaluating the behavior flag data with the computer system (*pages 1 - 2, Abstract; the expert system ASAX analyzes the emulator data*).

5.3. Regarding claim 13:

5.3.1. Le Charlier teaches initializing the virtual machine within the computer system, the virtual machine comprising a virtual computer implemented by software simulating functionality of a central processing unit and memory and a virtual operating system simulating functionality of an operating system of the computer system (*pages 13 - 15, sections 4.4 - 4.6*).

5.4. Regarding claim 14:

5.4.1. Le Charlier does not specifically teach identifying a type of operating system intended for the target program that is to be executed by the virtual machine.

5.4.2. Custer teaches identifying a type of operating system intended for the target program that is to be executed by the virtual machine (*pages 133 -135, section 5.2.2 Running Applications*).

5.5. Regarding claim 15:

5.5.1. Le Charlier does not specifically teach initializing the virtual machine by constructing the virtual machine out of a number of layered shells.

5.5.2. Custer teaches initializing the virtual machine by constructing the virtual machine out of a number of layered shells (*page 150, figure 5-17*).

5.6. Regarding claim 16:

5.6.1. Le Charlier does not specifically teach configuring the shells based upon a format of the target program.

5.6.2. Custer teaches configuring the shells based upon a format of the target program (*pages 133 -135, section 5.2.2 Running Applications*).

5.7. Regarding claim 18:

5.7.1. Le Charlier teaches loading a software CPU shell when the virtual machine operates in the first and third modes of operation (*page 13, section 4.4; and page 2, section 1 Introduction, paragraph 4, last sentence*).

5.8. Regarding claim 19:

5.8.1. Le Charlier does not specifically teach loading a language interpreter when the virtual machine operates in the second mode of operation.

5.8.2. Chi teaches loading a language interpreter when the virtual machine operates in the second mode of operation (*figure 1; figure 3; figure 4; and column 1, lines 45 - 58; and column 5, lines 20 - 50*).

5.9. Regarding claim 20:

5.9.1. Le Charlier teaches a processing unit (*page 15, figure 4*).

5.9.2. Le Charlier teaches a memory storage device (*page 15, figure 4; it would have been obvious that UNIX is stored in a memory storage device*).

5.9.3. Le Charlier teaches one or more program modules stored in said memory storage device for providing instructions to said processing unit (*page 15, figure 4; it would have been obvious that UNIX is stored in a memory storage device for providing instructions to the CPU processing unit*).

5.9.4. Le Charlier teaches a processing unit executing instructions of one or more program modules operable for:

5.9.4.1. Refer to the elements discussed under the teachings of Le Charlier in claim 11 above.

5.9.4.2. evaluating the behavior flag data and sequence flag data with the computer system (***pages 1 – 2, Abstract; the expert system ASAX analyzes the emulator data***).

5.9.5. Le Charlier does not specifically teach:

5.9.5.1. evaluating a file format of the target program.

5.9.5.2. evaluating control fields within a header of a file containing the target program.

5.9.5.3. automatically configuring the virtual machine to execute the target program in one of three modes of operation based on the file format and the control fields within the header of the file, a first mode of operation comprising a real mode, a second mode of operation for executing target programs comprising a high level programming language, and a third mode of operation comprising a protected mode for executing target programs comprising thirty-two bit code.

5.9.6. Custer teaches:

5.9.6.1. Refer to the elements discussed under the teachings of Custer in claim 11 above.

5.9.7. Chi teaches:

5.9.7.1. Refer to the elements discussed under the teachings of Chi in claim 11 above.

5.10. Regarding claim 21:

5.10.1.1. Refer to the elements discussed under the teachings of Le Charlier in claim 11 above.

5.11. Regarding claim 22:

5.11.1. Le Charlier teaches the virtual machine comprising a virtual computer implemented by the one or more programs simulating functionality of a central processing unit and memory and a virtual operating system simulating functionality of an operating system of the computer system (***pages 13 - 15, sections 4.4 - 4.6***).

5.12. Regarding claim 23:

5.12.1. Le Charlier does not specifically teach identifying a type of operating system intended for the target program that is to be executed by the virtual machine.

5.12.2. Custer teaches identifying a type of operating system intended for the target program that is to be executed by the virtual machine (***pages 133 -135, section 5.2.2 Running Applications***).

5.13. Regarding claim 24:

5.13.1. Le Charlier does not specifically teach initializing the virtual machine by constructing the virtual machine out of a number of layered shells.

5.13.2. Custer teaches initializing the virtual machine by constructing the virtual machine out of a number of layered shells (***page 150, figure 5-17***).

5.14. Regarding claim 25:

5.14.1. Le Charlier does not specifically teach configuring the shells based upon a format of the target program.

5.14.2. Custer teaches configuring the shells based upon a format of the target program (*pages 133 -135, section 5.2.2 Running Applications*).

5.15. Regarding claim 27:

5.15.1. Le Charlier teaches loading a software CPU shell when the virtual machine operates in the first and second modes of operation (*page 13, section 4.4; and page 2, section 1 Introduction, paragraph 4, last sentence*).

5.15.2. Le Charlier does not specifically teach loading a software CPU shell when the virtual machine operates in the first *and second* modes of operation.

5.15.3. Chi teaches loading a software CPU shell when the virtual machine operates in the *second* mode of operation (*figure 4, element 15*).

5.16. Regarding claim 28:

5.16.1. Le Charlier does not specifically teach loading a language interpreter when the virtual machine operates in the second mode of operation.

5.16.2. Chi teaches loading a language interpreter when the virtual machine operates in the second mode of operation (*figure 1; figure 3; figure 4; and column 1, lines 45 - 58; and column 5, lines 20 - 50*).

5.17. Regarding claim 29:

5.17.1. Le Charlier teaches:

5.17.1.1. Refer to the elements discussed under the teachings of Le Charlier in claim 11 above.

5.17.2. Le Charlier does not specifically teach:

5.17.2.1. automatically configuring a virtual machine to execute the target program in one of three modes of operation, a first mode of operation comprising a real mode, a second mode of operation for executing a target program comprising a high level programming language, and a third mode of operation comprising a protected mode for executing target programs comprising thirty-two bit code.

5.17.3. Custer teaches:

5.17.3.1. Refer to the elements discussed under the teachings of Custer in claim 11 above.

5.17.4. Chi teaches:

5.17.4.1. Refer to the elements discussed under the teachings of Chi in claim 11 above.

5.18. Regarding claim 30:

5.18.1. Le Charlier does not specifically teach evaluating a file format of the target program.

5.18.2. Refer to the elements discussed under the teachings of Custer in claim 11 above.

6. Claims 17 and 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Le Charlier, and Custer and Chi, in view of Nachenberg (U.S. Patent 6,851,057)

6.1. Regarding claims 17 and 26:

6.1.1. Le Charlier does not specifically teach that the virtual machine executes the target program starting at each entry point defined within an entry point table.

6.1.2. Nachenberg teaches that the virtual machine executes the target program starting at each entry point defined within an entry point table (***column 2, lines 28 - 32; and column 2, lines 55 - 59***).

6.1.3. The motivation to use the art of Nachenberg with the art of Le Charlier is the benefit recited in Nachenberg of providing a method to detect the presence of a virus in a file having multiple entry points (*column 2, lines 28 - 32; and column 2, lines 55 - 59*).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Russ Guill whose telephone number is 571-272-7955. The examiner can normally be reached on Monday - Friday 9:00 AM - 5:30 PM.

8. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Leo Picard can be reached on 571-272-3749. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Any inquiry of a general nature or relating to the status of this application should be directed to the TC2100 Group Receptionist: 571-272-2100.

9. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RG

LEO PICARD
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100